UNITED STATES DISTRICT COURT

WESTERN DISTRICT OF NEW YORK

- - - - - - - - - - - - - - - -X

UNITED STATES OF AMERICA 18-CR-6094(G)

vs.

Rochester, New York

CARLOS JAVIER FIGUEROA, June 1, 2021

Defendant. 9:03 a.m.

- - - - - - - - - - - - - - - -X

TRANSCRIPT OF TESTIMONY OF SCOTT FERRO
BEFORE THE HONORABLE FRANK P. GERACI, JR.
UNITED STATES DISTRICT CHIEF JUDGE

JAMES P. KENNEDY, JR., ESQ.
United States Attorney
BY: ROBERT A. MARANGOLA, ESQ.
CASSIE M. KOCHER, ESQ.
Assistant United States Attorneys
500 Federal Building
Rochester, New York 14614
Appearing on behalf of the United States

PAUL J. VACCA, JR., ESQ.
One East Main Street, Suite 1000
Rochester, New York 14614
Appearing on behalf of the Defendant

ALSO PRESENT: Gabriela Loncar, Spanish Interpreter
James Hontoria, Spanish Interpreter

COURT REPORTER: Christi A. Macri, FAPR-RMR-CRR-CSR(NY/CA)
Christimacri50@gmail.com
Kenneth B. Keating Federal Building
100 State Street, Room 2640
Rochester, New York 14614

I N D E X

WITNESS FOR THE GOVERNMENT

P R O C E E D I N G S

* * *

(WHEREUPON, the defendant is present).

CROSS-EXAMINATION

09:03:37AM **BY MR. VACCA:**

Q. Investigator, do you have the extraction book up there with you?

A. No.

Q. Do you have copies of your extractions?

09:03:48AM A. No.

MS. KOCHER: Mr. Vacca, we can pull them up on the Trial Director.

MR. VACCA: Okay, that's fine.

MS. KOCHER: If you want to direct us to one in

09:03:56AM particular.

MR. VACCA: Yes, 669A.

BY MR. VACCA:

Q. Investigator, do you see on the board there 669A?

A. Yes.

09:04:19AM Q. Okay. And did you do the extraction report on that?

A. Did I run this report? Or print it out?

Q. Print it out.

A. I did not print this out, no.

Q. Did you run -- did you run the extraction?

09:04:32AM A. Yes.

Q. On this particular phone?
A. Yes.
Q. How many extractions and how many phones did you run?
A. On this case?
09:04:41AM Q. Yes.
A. I'm not sure.
Q. Okay. Do you have a guess at the numbers?
A. Over 30.
Q. Over 30?
09:04:51AM A. Yes.
Q. Okay. And most of them did you have a search warrant for?
A. Yes.
Q. For each and every phone?
A. I believe all except for two which were consent.
09:05:03AM Q. Consent? In other words, you obtained consent of the owner of that phone to do a search of the phone?
A. Correct.
Q. All right. With respect to 669A, if you take a look at the summary, what does the summary contain?
09:05:22AM A. That is information based on the computer that's used for the extraction.
Q. In this particular one did you run the extraction on 5/2 of 2021?
A. No, that's the created time of the report.
09:05:38AM Q. That's when the report's printed out?

A. Correct.
Q. All right. When did you do the actual extraction on this -- on this phone?
A. October -- looks like October 5th.
09:05:52AM Q. Okay. Of 2020?
A. Yes.
Q. Now, what -- what is an external camera media? Is that section information relevant to an extraction of a camera or other media on that particular cell phone?
09:06:12AM A. No, that is the -- it's called a UFED camera, which is a camera that I had hooked up to the extraction machine that will take photographs or video of the phone.
Q. A along with information related to that such as phone number calling or individual calling?
09:06:32AM A. It will record whatever I open the phone to.
Q. Okay. And then we have file system. What does file system mean?
A. So file system is a type of extraction. There's basically three types of extraction. File system is taking the phone
09:06:51AM and going through each individual file looking to binary code and then extracting the binary code and then translating that.
Q. What does binary code mean?
A. Zeros and ones.
Q. Zeros and ones?
09:07:09AM A. Yes.

Q. Again could you explain that a little better?
A. So everything -- a phone is like a computer. Everything on that phone is just in binary. Just zeros and ones. And then it gets translated to hexadecimal and then ASCII, which is basically how you read, how you are able to view the information.
Q. That's what takes the information out of the phone and either prints it out or puts it on a phone screen?
A. Yes, just takes the ones and zeros, correct.
09:07:41AM Q. All right. And in this particular extraction on 669A, were you told by anybody -- your superior, your supervisor or whatever, what you were looking for with this particular extraction on 669A?
A. No, I just pull the information.
09:07:59AM Q. Whatever was there was there?
A. Correct.
Q. And then you printed it out?
A. I provided it in the electronic form. I did not print out this report.
09:08:10AM Q. Is the electronic the same as the printed copy?
A. No.
Q. It's different?
A. So the initial -- so there's two different kinds of electronic files that I provide. One would be the report copy
09:08:26AM which you find right here; and the other one is the binary

code.
Q. What's the binary code?
A. The ones and the zeros.
Q. The ones -- but I still don't understand what ones and zeros mean.
09:08:37AM
A. So that's the program that it's written in. Everything that you see on any computer in your phone is just ones and zeros stored on a computer chip.
Q. What does that -- what if you have something that's number three or four?
09:08:54AM
A. So there's a combination of ones and zeros; when you read the ones and zeros, it says three or four.
Q. It says three or four?
A. Correct. When you translate it back from binary to what is referred to as ASCII, which is your characters that you are able to see.
09:09:09AM
Q. Okay. So what's ASCII?
A. A-S-C-I-I, American Standard -- I forget the last three -- it's your -- basically your letters and numbers in English that you are able to view.
09:09:31AM
Q. What does it tell us about the phone?
A. Doesn't tell us anything about the phone. It's what you're able to see. When, for instance, the text message is -- those are characters. Those characters are not really on the chips of the phone. It's the ones and zeros that are
09:09:50AM

on the phone that show what those characters are.
Q. I'll give you an example: Do you have -- do you have on there where it says logical?
A. Yes.
09:10:04AM Q. What's logical?
A. So logical extraction is just basically looking at the phone, how you see it in going through text messages, contacts, it's basically going through each category that you see on the phone whereas opposed to a file system which goes
09:10:23AM through each file and looks at the ones and zeros.
Q. Okay. And with respect to 669A under logical you've got unit identifier, correct?
A. Yes.
Q. And numbers 853371537, what do those numbers mean?
09:10:41AM A. That is my key for my license for Cellebrite.
Q. I don't understand. Your key?
A. Yes, so Cellebrite, it's a proprietary product. I need to have permission to use it. I have what's called a dongle that plugs into the side of the machine that shows my license is
09:11:05AM up-to-date and paid for.
Q. Now, you analyzed this on what date? You extracted on 10/5/2020?
A. Yes.
Q. 10/5/2020. Do you know when that phone was -- was seized
09:11:25AM as a result of a search warrant ?

A. Do I know? No, no, not off the top of my head. I don't know.
Q. This was analyzed October 5th, 2020, correct?
A. Yes.
09:11:39AM Q. Okay. But nowhere on this form does it say when this phone was seized during a search warrant or it came into your possession, correct?
A. Correct.
Q. You were just asked some time in October of 2005 to
09:11:55AM analyze this, correct?
A. Of 2020.
Q. 2020, excuse me.
A. Yes.
Q. What is -- what is logical?
09:12:04AM A. The logical is the type of -- is a type of extraction.
Q. Okay. And could you explain to us in further detail what type of extraction there is with logical?
A. So logical looks at what you can see on the phone. If you were to open up your phone and go through your contacts, your
09:12:24AM text messages, anything that you can see, that's what it's going to give you.
Q. Okay. And what's the difference between a full extraction and a partial extraction?
A. So a partial extraction would only get part of the
09:12:40AM information. There's full logicals, there's partial logicals.

It depends on a lot of times the phone model. If the phone has been updated there's all kinds of factors that depending that would influence getting everything off of the phone.

Q. Well, with 669A as an example, was that a full extraction or a partial extraction?

09:13:07AM

A. So I'd have to look at my notes to see if it was a full or partial extraction. But I would imagine this is only going to be a partial extraction only because I used the UFED camera to extract some other stuff.

Q. So you can't tell by looking at this report if you did a partial or a full extraction?

09:13:27AM

A. Correct. That's correct, I need my extraction -- the written extraction report.

Q. Okay. And if it was a partial extraction, do you know what information would be left off of this report?

09:13:42AM

A. From looking at this, no, I wouldn't. I wouldn't know.

Q. You wouldn't know?

A. No.

Q. Do you have notes somewhere that would tell you on all of these extractions whether or not they're full or partial?

09:13:55AM

A. I have my handwritten extraction report, yes.

Q. Okay. And as far as the report is concerned, you don't know if you left something out in analyzing the phone if it's a partial?

A. The information is there. Whether it's decoded or not is

09:14:17AM

what sometimes is problematic.
Q. Who decides what gets decoded?
A. So some of it is the company, Cellebrite. Some of it it doesn't decode. Some I'm able to decode for it. And other
09:14:39AM times it's just, you know, the technology, for instance, there's lots of apps that come out after the phones are initially made. So these apps could effect how the phones function.
Q. Well, this arrest was made -- several of the arrests with
09:15:00AM respect to the cell phones were made in January of 2018; is that correct?
A. Yes.
Q. And with many of them your analysis didn't take place until sometime in 2020, correct?
09:15:14AM A. Yes.
Q. Okay. So we're talking almost two years that those phones sat unexamined?
A. Yes.
Q. Okay. What effect would that have on your decoding or
09:15:30AM analysis in, let's say, October 2020 with the upgrades that there were with the phone and the alterations there were with the program?
A. It would generally give us more information now than it did in 2018.
09:15:47AM Q. In 2018 did you examine this phone and generate a phone

like in 669A?
A. I'm not sure if that's one I did in 2018 or not.
Q. Do you know how many you did in 2018?
A. I don't.
09:16:03AM Q. Okay. So you don't know on many of these if you got a partial extraction?
A. If I looked at my written notes I would know if it was a partial or full extraction, yes.
Q. So a partial extraction leaves something out, correct?
09:16:18AM A. Correct.
Q. Okay. And a full extraction, does that leave something in?
A. Does it leave something in? In the phone?
Q. Yeah, in the phone.
A. So how the extraction works normally is it's going to load
09:16:33AM a program on to the phone and then take the program off of the phone when the extraction is over with. So it should not leave anything on the phone. However, you will be able to tell that a program was loaded on to it.
Q. Okay. And was there a program loaded on this one?
09:16:52AM A. Yes.
Q. And was it a program from 2018 or was it a program from October 2020?
A. From 2020.
Q. Okay. So we don't know if the report would have been from
09:17:04AM 2018, correct?

A. I'm sorry?
Q. You -- we wouldn't know what the report said if it was extracted in 2018?
A. If I did an extraction on this phone in 2018, it was provided.
Q. Okay. And, again, with all of these phones -- and there are several of them -- were you -- were you told by somebody, one of your superiors again or whatever, what to look for on the extraction?
A. No, I just pulled all the information from the phone and put it into a readable format.
Q. Could you tell us how long it took to extract on this phone?
A. This one is fairly quick. Looked like just a minute.
Q. Just a minute?
A. Yeah.
Q. So that means that it did not extract a lot of information?
A. Or there was not a lot of information there, yes.
Q. Okay. In October 2020, correct?
A. Correct.
Q. But in January of 2018 there's a possibility that it may have extracted more information, correct?
A. Possibly.
Q. Or less?

A. Correct.
Q. Because a program changes, right?
A. Right.
Q. Do you know what program changes there were between 2018 and 2020?
A. There were several updates between that time. Several.
Q. Okay. Now, looking at 669A, if you turn the page it has contacts, correct?
A. Yes.
Q. And it has plug-ins, right?
A. Yes.
Q. What is a plug-in?
A. That's just -- that's basically our program, the Cellebrite program.
Q. The plug-in?
A. Right.
Q. Okay.
A. Yes.
Q. So after -- after you do a summary and a source extraction -- that's external camera media, file system, logical, then you go to plug-ins, right?
A. That's a category on the summary, yes.
Q. Now, on the summary here you have -- you have a number of things and like I just said, summary, source extraction, file system. Is that how they run in terms of one after the other

or are they rearranged after you finish the full extraction?
A. So I -- I do -- generally I'll do a logical extraction first and then a file system. This is how it prints out. This is the format that it prints out in, yes.
09:19:52AM Q. It rearranges everything?
A. It puts it into a readable format.
Q. Okay. So you put it in -- what do you do first, logical?
A. Generally I'll do a logical first, yes.
Q. Is there a reason for that?
09:20:04AM A. It's faster.
Q. It's faster?
A. It's faster, yes.
Q. Do you miss any information that way?
A. There's -- it doesn't pull all the information -- a
09:20:15AM logical does not pull all the information off the phones.
Q. On all these phones there is something that is left and not included in the report, correct?
A. No.
Q. No? Everything is taken off the phone?
09:20:29AM A. If you do a physical or a file system extraction everything is taken off the phone. It might not be decoded, but everything is taken off the phone.
Q. Was it -- on this particular one was it decoded?
A. It was not.
09:20:43AM Q. It was not decoded?

A. Correct.
Q. So what does that mean?
A. So everything in the files was not necessarily decoded by Cellebrite.
09:20:56AM Q. What effect does that have on your total analysis of this phone?
A. Doesn't really have any effect on it.
Q. But you're leaving information behind?
A. Information is there. A lot of it is -- could be just the
09:21:18AM workings of the phone. You know, your internal clock workings telling the phone how it operates. So that stuff is not decoded by the program.
Q. Okay. Is there also something called preprogramming?
A. So there's things that are programmed onto your phone,
09:21:42AM yes, before you take it out of the box.
Q. And if you take a look at the next page, it's under contacts, I think there's 15 contacts.
A. Yes.
Q. Okay. Why don't you explain to us and to the jury what
09:21:56AM that means?
A. The 15 contacts?
Q. Yes. What does a contact mean?
A. A contact is a stored number or name or some kind of information in your phone.
09:22:12AM Q. Okay. Some of these extractions have like 300, 320,

correct?
A. Oh, yes.
Q. Those are all stored in the phone?
A. Yes.
09:22:21AM Q. Phone numbers that are stored in the phone?
A. Yes.
Q. Do we know how they got there?
A. Somebody would have to input them into the phone.
Q. So in other words, if I have my phone and I want to put
09:22:33AM your phone number in, what's your phone number, I go like this and I put it in my phone?
A. Yes.
Q. Okay. So we have to hand load it into the phone, correct?
A. Yes.
09:22:43AM Q. Are there also other times when you just use the phone and call that number, all right? Is that loaded in the phone?
A. Is it stored and saved as a contact?
Q. Yes.
A. If you just dial that phone number?
09:22:57AM Q. Yes.
A. No, it's not -- it's in the phone, but it's not stored as a contact.
Q. So of all these phones that we have, some of them with 300 contacts, which may have a phone number in it of someone who
09:23:13AM they show us on that chart, okay? Of people who they feel are

involved in all these phone calls, those phone calls, okay? Were not calls made from that phone because they're not loaded into the phone, correct?

MS. KOCHER: Objection.

09:23:28AM **THE COURT:** Overruled. If he understands the question.

THE WITNESS: No. You can call a number without having it loaded into the phone.

BY MR. VACCA:

09:23:40AM Q. Okay. So let's say there's, you know, one of these contacts (sic) that has 200 contacts, okay? By you taking a look at the printout on the contacts, could you tell what phone number called this phone at 669A?

A. So there are some phones that I did the extractions on

09:24:06AM that when you pulled the contacts it says how many times it contacted another number.

Q. A specific number?

A. Yes.

Q. Okay. But then there's some that don't tell you that

09:24:20AM specific number, correct?

A. Correct.

Q. That was contacted?

A. Correct.

Q. And looking at the numbers here, did you look at all the

09:24:30AM contact numbers on all these phones?

A. No.
Q. So I don't know what ones were loaded in or which ones came from phone calls, correct?
A. The phone calls -- that would be a separate category. That's not contacts.
Q. Okay. So do you also have phone calls that you're able to extract?
A. Yes, call logs, yes.
Q. It's called a call log?
A. Yes.
Q. Okay.

MR. VACCA: If I may just have one minute, Your Honor?

THE COURT: Sure.

BY MR. VACCA:

Q. Investigator, have you ever had failed extractions?
A. Yes.
Q. Why don't you tell the jury what failed extractions are?
A. It's just an extraction that doesn't happen, it doesn't work, whether it's the phone could be broke, it could not be recognizing the system, there could be a program loaded on to the phone that's preventing the extraction.

Sometimes some cell companies load programs onto their phones to prevent you from switching your phone to another provider. That will hamper an extraction sometimes

and you would have to take that off or disable it before you can get an extraction.

Sometimes phones are dead and not able to be powered on. If you can't get power into the phone, sometimes you cannot get an extraction. So there's several factors that could hamper an extraction.

MR. VACCA: Thank you very much, Investigator.

THE WITNESS: Thank you.

REDIRECT EXAMINATION

BY MS. KOCHER:

Q. Investigator Ferro, Mr. Vacca was asking you about Exhibit 669A. Asked you whether or not it was a full or partial extraction. You mentioned you have some notes regarding that?

A. Yes.

MS. KOCHER: Your Honor, may I approach the witness?

THE COURT: Yes.

BY MS. KOCHER:

Q. Investigator, I've handed you what's been marked for identification purposes as Exhibit 836. Do you recognize that document?

A. Yes.

Q. What is that?

A. This is my extraction form. These are the handwritten notes that I took in regards to this phone 669.

Q. Okay. And that's a one-page document?
A. Yes.
Q. If you'd like to take a look at that and let me know if that refreshes your recollection as to whether or not this is a full or a partial extraction?
A. Yes.
Q. Okay. Are you able to tell?
A. Yes.
Q. What was it?
A. So it was a full logical, a full file system. However, it did not decode a lot of the information. So I used the UFED camera to take pictures of what it did not decode.
Q. Okay. And if we could turn to the fifth page of the extraction report, 669A? Some of those pictures that you took --
A. Yes.
Q. -- to get that additional data wasn't decoded?
A. Yes.
Q. Now, you also talked with Mr. Vacca about binary code?
A. Yes.
Q. And that's the number zeros and ones?
A. Correct.
Q. Is Cellebrite, does that take those binary codes and translates it into a readable format?
A. Yes, it takes it -- I'm able to view it in hexadecimal and

then it gives you your extraction report that you're able to read, yes.

Q. Okay. And has technology changed since 2018?

A. Yes.

09:28:34AM Q. Generally are you able to get more information from extractions now than you were two years ago?

A. Yes.

Q. I guess three years ago at this point?

A. Correct.

09:28:45AM Q. When you're performing extractions do you add anything to the extraction report that was not on the phone?

A. No.

Q. Are you able to alter any of the contents of the phone?

A. No.

09:29:01AM **MS. KOCHER:** Thank you, Investigator.

THE WITNESS: Thank you.

MR. VACCA: No recross, Your Honor. Thank you.

THE COURT: You may step down. Thank you very much.

09:29:07AM **THE WITNESS:** Thank you, Your Honor. Thank you.

(**WHEREUPON**, the witness was excused).

* * *

CERTIFICATE OF REPORTER

In accordance with 28, U.S.C., 753(b), I certify that these original notes are a true and correct record of proceedings in the United States District Court for the Western District of New York before the Honorable Frank P. Geraci, Jr. on June 1st, 2021.

S/ Christi A. Macri

Christi A. Macri, FAPR-RMR-CRR-CSR(CA/NY)
Official Court Reporter